REMARKS:

Claims 42 and 43 are canceled without prejudice or disclaimer. Claim 44 is newly added. Claims 21, 23, 25, 26 and 29-41 are amended as indicated in the preceding pages. No new matter is added.

In view of the above-noted claim amendments, claims 21-23, 25, 26, 29-41 and 44 are currently pending, with claims 21, 29 and 40 being independent claims.

The Examiner rejected claims 21, 22, 25, 26, 29, 30 and 32-39 under 35 U.S.C. §102(e) as being anticipated by *Chen et al.* (U.S. Patent Application Publication No. 2004/0233910, referred to below as "*Chen*"). *See pp. 4-6 of the Final Office Action.* The Examiner rejected claims 23 and 31 under 35 U.S.C. §103(a) unpatentable over *Chen* in view of *Rabe et al.* (U.S. Patent No. 7,194,538, referred to below as "*Rabe*"). *See pp. 6-7 of the Final Office Action.* The Examiner rejected claims 40-43 under 35 U.S.C. §102(b) as being anticipated by *Iwatani* (U.S. Patent Application Publication No. 2001/0054093). *See pp. 7-9 of the Final Office Action.* These rejections are respectfully disagreed with and are traversed below. The Applicants respectfully request reconsideration and further examination of the present application under 37 C.F.R. §1.114.

As to the rejection of claim 21, the Applicant has thoroughly considered the Examiner's remarks concerning *Chen*. To warrant the §102(e) rejection claim 21, *Chen* must teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. *See MPEP §706.02(V).* The Applicant respectfully traverses this §102(e) rejection of claim 21 because *Chen* fails to teach all of the limitations of amended independent claim 21.

Amended claim 21 recites:

> A computer-implemented method comprising:

managing a storage area network (SAN) with at least a SAN Management server and a SAN Management client, said SAN Management client running a trusted operating system and having a communication path to a Fibre Channel adapter, said Fibre Channel adapter being disposed between the SAN and at least one computer system running an untrusted operating system, said SAN Management server being connected to the at least one computer system and the SAN Management client, said SAN Management client being further connected to the at least one computer system, and

separating requests issued by the SAN Management server into at least two groups,

where a first group of requests is issued to the SAN Management client and processed by the Fibre Channel adapter and the SAN on behalf of the SAN Management client in place of the at least one computer system, and

a second group of requests is issued to and processed by the at least one computer system without the need to send or receive requests to or from the Fibre Channel adapter and the SAN.

The arrangement of the various components recited in claim 21 is similar to that shown in FIG. 1 of the instant application. As recited in claim 21, requests issued by the SAN Management server (e.g., 130) are separated into at least two groups with a first group being issued to the SAN Management client (e.g., 132) and a second group being issued to the at least one computer system (e.g., 104, 105, 106). The at least one computer system is running an untrusted operating system. The first group of requests is processed by the Fibre Channel adapter (e.g., 112) and the SAN (e.g., 110) on behalf of the SAN Management client in place of the untrusted at least one computer system, thus limiting access to the SAN by the untrusted at least one computer system. That is, because the SAN Management client has a trusted operating system it is allowed to communicate requests for (i.e., in place of or instead of) the untrusted at least one computer system. As non-limiting examples, the first group of requests may comprise authorized SAN access requests and the second group of requests may comprise operating system configuration requests.

Chen differs from the computer-implemented method recited in claim 21 in a number of ways. First, *Chen* does not disclose or suggest "separating requests issued by the SAN Management server into at least two groups, where a first group of requests is issued to the SAN Management client and processed by the Fibre Channel adapter and the SAN **on behalf of the SAN Management client in place of the at least one computer system**" as recited in claim 21. In contrast to claim 21, in the system of *Chen* an untrusted operating system or relationship is not allowed to persist and communicate. In *Chen*, if a client is determined not to be verified/authenticated ("NO" in block 555 of FIG. 5), the client is verified and authenticated prior to connection with the storage server. If verification fails for a request, a generic reply is transmitted without enabling access to the device (see block 630 of FIG. 6).

In contrast to *Chen*, claim 21 recites that the "first group of requests is issued to the SAN Management client and processed by the Fibre Channel adapter and the SAN **on behalf of the SAN Management client in place of the at least one computer system.**" This allows the SAN Management client to communicate with the Fibre Channel adapter and SAN in place of the untrusted at least one computer system. Furthermore, requests and results from this communication can be propagated to the untrusted at least one computer system. *See, e.g., FIG. 5 of the instant application*. *Chen* does not disclose or suggest using a trusted intermediary (e.g., the SAN Management client) in such a manner.

One example of an advantage provided by "separating requests issued by the SAN Management server into at least two groups, where a first group of requests is issued to the SAN Management client and processed by the Fibre Channel adapter and the SAN **on behalf of the SAN Management client in place of the at least one computer system,**" as recited in claim 21, is that requests can be propagated by the SAN Management client on behalf of the at least one computer system. Thus, even though the at least one computer system is running an untrusted operating system, requests on the SAN can be issued and processed since the SAN Management client, known to be running a trusted operating system, issues such requests "**in place of the at least one computer system.**"

Second, *Chen* does not disclose or suggest "**separating requests issued by the SAN Management server into at least two groups**" as recited in claim 21 of the instant application. *Chen* discloses a number of groupings such as local/remote, FC/SCSI and SAN/NAS, however, none of the groupings disclosed by *Chen* are similar to those recited in claim 1 since none of the groupings allows a first group to be processed by an adapter and storage network/device on behalf of a trusted entity in place of another untrusted entity ("issued to the SAN Management client and processed by the Fibre Channel adapter and the SAN on behalf of the SAN Management client in place of the at least one computer system" as recited in claim 21) with a second group processed by the untrusted entity without the need to send or receive requests to or from the adapter and the storage network/device ("issued to and processed by the at least one computer system without the need to send or receive requests to or from the Fibre Channel adapter and the SAN" as recited in claim 21).

Third, in the system of *Chen* no trusted operating system or relationship is initially present. As is apparent from blocks 555, 560, 615 and 620 in FIGS. 5 and 6, *Chen* inquires whether the client/request is verified/authenticated. This is in contrast to "said SAN Management client running a **trusted operating system**," as recited in claim 21, wherein the SAN Management client is known to have a trusted operating system. Furthermore, this is also in contrast to "at least one computer system running an **untrusted operating system**," as recited in claim 21, wherein the at least one computer system is known to have an untrusted operating system.

One example of an advantage provided by "said SAN Management client running a **trusted operating system**" and "at least one computer system running an **untrusted operating system**," as recited in claim 21, is that no initial authentication or validation need be performed. If the SAN Management client is known to run a trusted operating system, there is no need to authenticate or verify the other computer systems (i.e., the "at least one computer system running an untrusted operating system"). The valid authorization checks illustrated in FIG. 3 (blocks 312 and 321) are in regards to security as opposed to a determination regarding whether or not a given operating system on a given entity is trusted or untrusted.

In paragraph [0013], *Chen* discloses two types of requests: those that are communicated to the storage device and those that are answered by the storage server instead of the storage device (e.g., a type of status request). However, the storage server does not process the requests on behalf of a client in place of another untrusted computer system. Thus, the storage server does not correspond to the SAN Management client recited in claim 21. The storage server does not issue requests and so it cannot be seen to correspond to the SAN Management server recited in claim 1. Furthermore, the storage server of *Chen* is allowed to directly communicate with the storage device (without an intermediary) and, thus, cannot be seen to correspond to the untrusted at least one computer system recited in claim 21.

As is apparent, the storage server described by *Chen* does not correspond to any of the entities recited in claim 21 of the instant application. This is because the fundamental architecture of the system of *Chen* (e.g., the presence and arrangement of entities) is different from that recited in claim 21. As noted above, *Chen* does not provide for a trusted intermediary (the SAN Management client) to act in place of an untrusted entity (the at least one computer system).

Based on the above, it is clear that *Chen* does not disclose or suggest: "A computer-implemented method comprising: managing a storage area network (SAN) with at least a SAN Management server and a SAN Management client, said SAN Management client running a trusted operating system and having a communication path to a Fibre Channel adapter, said Fibre Channel adapter being disposed between the SAN and at least one computer system running an untrusted operating system, said SAN Management server being connected to the at least one computer system and the SAN Management client, said SAN Management client being further connected to the at least one computer system," as recited in claim 21.

Furthermore, *Chen* does not disclose or suggest "separating requests issued by the SAN Management server into at least two groups, where a first group of requests is issued to the SAN Management client and processed by the Fibre Channel adapter and the SAN on behalf

of the SAN Management client in place of the at least one computer system, and a second group of requests is issued to and processed by the at least one computer system without the need to send or receive requests to or from the Fibre Channel adapter and the SAN," as recited in claim 21.

It is briefly noted that neither *Rabe* nor *Iwatani*, considered separately or in combination, said combination not being admitted to as feasible and/or practicable, remedy the above-noted defects of *Chen*.

The features recited in claim 21 are not disclosed or suggested in the cited art. *Chen* does not anticipate claim 21 and, therefore, claim 21 is patentable and should be allowed.

Though dependent claims 22, 23, 25 and 26 contain their own allowable subject matter, these claims should at least be allowable due to their dependence from allowable claim 1.

Independent claims 29 and 40 claim similar features as claim 1 noted above. For the same reasons stated above with respect to claim 21, independent claims 29 and 40 are not anticipated by *Chen*. Therefore, claims 29 and 40 are patentable and should be allowed.

Though dependent claims 30-39, 41 and 44 contain their own allowable subject matter, these claims should at least be allowable due to their dependence from allowable independent claims 29 and 40.

The Applicant respectfully reserves the right to argue one or more of the dependent claims in a future communication or response. For example, since *Chen* does not utilize a similar system architecture as exemplary embodiments of the instant application, and as recited in claims 21, 29 and 40, *Chen* may not be seen to disclose or suggest further aspects of such a system, such as those recited in claims 32-35, as non-limiting examples.

SUMMARY:

The Examiner is respectfully requested to reconsider and remove the rejections of claims 21-23, 25, 26 and 29-41 and to allow all of the pending claims 21-23, 25, 26, 29-41 and 44 as now presented for examination. For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record. Should any unresolved issue remain, the Examiner is invited to call Applicants' agent at the telephone number indicated below.

Respectfully submitted:

Alan L. Stern — December 26, 2008

Alan L. Stern
Date

Reg. No.: 59,071

Customer No.: 49132

HARRINGTON & SMITH, PC
4 Research Drive
Shelton, CT 06484-6212
Telephone: (203) 925-9400 ext. 18
Facsimile: (203) 944-0245
E-mail: astern@hspatent.com